ISSA Fall 2009 Seminar (Two for One)

When: Thursday, 1 October 2009; 9am – 5pm (check-in starts at 8am)

Where: SLCC Miller Conference Center (see map for directions)

Topic: Data Loss Prevention

Food: Morning and afternoon breaks, full buffet lunch

Cost: ISSA and ISACA members: $100
Non-members: $200

Bring a Friend/Co-worker for Free
(One Paid Registration Equals Two Attendees)

Register: Online at the http://www.issa-utah.org (PayPal or check payment options; if you have questions send an email to treasurer@issa-utah.org)

Credit: 6 CPE Credits

Sponsors

Break Sponsor
- SafeNet/Aladdin

Tabletop Sponsors
- Accuvant
- ArcSight
- Code Green Networks
- Guidance Software
- PGP
- RSA
- SafeNet/Aladdin

Agenda:

8 Registration

9 Keynote: **Uzi Yair, CEO of GTB Technologies**
Topic: **Essential Elements of DLP System**

10 Break / Expo

10:30 Breakout Sessions A

#1 – ***Sensitive Data Detection: DLP Capabilities, Limitations, and Implications****;* Justin Searle, Joe Peck, Code Green, VP Product Management	#2 - ***SNORT in the Enterprise Security Infrastructure***; Brandon Greenwood – Xango

11:15 Breakout Sessions B

#3 – ***Social Networks - A Gateway to Your Company***; Justin Searle, Senior Security Analyst, InGuardians	#4 - ***Forensic Basics***; Fred Cotton – Guidance Software

12 Lunch / Expo

1:30 Keynote: **Matt Bossom, Director Wireless Security, Accuvant**
Topic: **DLP and Wireless Security**

2:30 Breakout Sessions C

#5 – ***Application Failures***; Mark Porter, Director of Systems Engineering, Breach Security	#6 - ***DLP in Theory and in Practice***; Pete Green, Novell

3:15 Break / Expo

3:45 Breakout Sessions D

#7 – ***DLP Emerging as a Critical Infosec Control Mechanism***; Mohan Atreya, Product Manager, RSA	#8 - SafeNet

4:30 Closing / Gifts

Keynotes

Uzi Yair is the co-founder and CEO of GTB Technologies; the only Data Loss Prevention Company to have solved the market limitation of high False Positive Rates. Uzi is responsible for setting the overall direction and product strategy for the company. Prior to GTB Technologies, Uzi was co- founder and CEO of Proxyconn Inc., the leading provider of Internet access acceleration solutions. Other assignments have been CEO of Redwood Software, CEO Magic Software Enterprises (North American division), a NASDAQ traded company , and CEO of Liant Software, a provider of 3GL development tools and technologies. Uzi holds an MBA from Columbia Business School along with a BS in Computer Science and Mathematics from Hofstra University.

Matthew Bossom is the Director of Wireless Solutions at Accuvant. Accuvant is a national security consulting organization that designs and executes strategies to address its clients' complex information security challenges. Matthew is responsible for providing leadership to Accuvant's wireless practice areas and offerings and ensures the ongoing world class capabilities of the Accuvant wireless security team. He has an track record of managing wireless projects and has a deep understanding of wireless systems, wireless network security, mobile computing, RF networks, spectrum analysis, RTLS and RFID solutions. Prior to joining Accuvant, Mr. Bossom served as a Wireless Security Product Manager at Accucode, Inc., a Wireless Systems Engineer at Barcoding, Inc., and a Network Infrastructure Project Manager for Inter-Tel Technologies, Inc.

Breakouts

Forensic Basics; Fred Cotton – Guidance Software

> An overview of computer forensics, including the forensic process, forensic protocols, before the case, opening a case, make a forensic copy, open and verify the disk image, hash / signature / entropy analysis, timeline analysis, process EFS and ID encrypted files, identify compound files, key word searching, process user data, bookmark and document findings.
>
> Fred Cotton is a Solutions Consultant assigned to the Emeryville, CA office. Prior to joining the team at Guidance Software, Fred was an Instructor with the Defense Computer Investigations Training Academy (DCITA). He was an Initial Responders-team instructor who researched and taught the Initial Responder's Course and the Forensic Examiner course. Fred also researches and writes on computer investigative and forensic related topics.

***Social Networks - A Gateway to Your Company*;** Justin Searle, InGuardians

> As the popularity of Social Networks grows, our employees are sharing personal information at an ever increasing pace. Whether to keep in contact with friends and family or to maintain their professional relationships, the information our employees are sharing not only affects their own privacy but also affects the privacy the companies they work for. The same

information that attackers use to attack these individuals can also be used to attack our companies. Join Justin Searle, a penetration tester from InGuardians, who has personally used these attacks to gain access to millions of credit cards and social security numbers on multiple accounts. This session will explore how employee use of Social Networks increase your company's risk of compromise and what you can do to mitigate these risks.

Justin Searle, a Senior Security Analyst with InGuardians, specializes in penetration testing and security architecture. Previously, Justin served as JetBlue Airway's IT Security Architect and has provided top-tier support for the largest supercomputers in the world. Justin has taught hacking techniques, forensics, networking, and intrusion detection courses for multiple universities and corporations. Justin has presented at top security conferences including DEFCON, ToorCon, ShmooCon, and SANS. Justin co-leads prominent open source projects including The Middler, Samurai Web Testing Framework, and the social networking pentest tools: Yokoso! and Laudnum. He is actively working to finish an new book *Social Network Attacks*, with Tom Eston of the Security Justice Podcast, and Kevin Johnson of InGuardians. Justin has an MBA in International Technology and is CISSP and SANS GIAC-certified in incident handling and hacker techniques (GCIH) and intrusion analysis (GCIA).

***Sensitive Data Detection: DLP Capabilities, Limitations, and Implications*; Joe Peck, Code Green, VP Product Management**

From keyword and regex matching to hash-based fingerprinting, DLP solutions use a wide range of techniques for detecting sensitive data, with varying levels of effectiveness. With so many vendors pitching DLP, exactly how a solution detects sensitive data should be part of your evaluation process. This session will discuss the most common methods, their capabilities, limitations, levels of false positives and negatives, evasion techniques, and implications for overall solution effectiveness.

***SNORT in the Enterprise Security Infrastructure*; Brandon Greenwood – Xango**

SNORT is an open source network intrusion prevention and detection system utilizing a rule-driven language, which combines the benefits of signature, protocol and anomaly based inspection methods. Snort is the most widely deployed intrusion detection and prevention technology worldwide. It has become the de facto standard for the industry. Brandon Greenwood, who formed the Utah SNORT users group, will be leading a discussion on the role SNORT plays in the modern enterprise security infrastructure. He will be discussing the following topics:

- Getting Snort in the door
- Uses of Snort (Packet Logger, IDS, IPS, etc)
- What open source (free) means when using Snort as your IDS/IPS
- Snort tools (user interfaces, automated alerting/signature updates, management, etc.)
- Tuning the application when used as an IDS/IPS

- Overview of what Snort 3.0 and how it will differ from 2.x

Brandon Greenwood, GSE, CISSP, CISM, GCFA, SnortCP. He holds a Bachelor of Science in Computer Science from Weber State University. He has worked in the security area for many years with special interest in strategic planning, policy, capital planning, IT governance, information security data management, and secure enterprise architecture. His background includes working in the public and private sectors filling various network and security related roles and responsibilities. In his spare time, Brandon formed and operates the Utah Snort Users Group and works with SANS as an OnDemand question writer and Technical Director. He is the Manager for Network Operations and Security for XanGo.

***Application Failures*; Mark Porter - Breach Security**

Application Failures – What information have you just given away and how can it affect your security.

Mark Porter is the Director of Systems Engineering at Breach Security. Mark is a seasoned professional with over 20 years of application development experience prior to moving into the security field. His combination of development and security expertise was instrumental in helping develop the company's Application Security Assessment program that are conducted at Fortune 100 companies and have helped hundreds of companies assess and remediate their application security.

***DLP Emerging as a Critical Infosec Control Mechanism* - Mohan Atreya - RSA**

DLP is emerging as a critical information security control mechanism. Organizations are deploying DLP to better control and protect sensitive data at the perimeter, data repositories, and at the endpoints. As these tools become mainstream within organizations, they will impact and challenge traditional views of data classification, protection and access controls. During this session, we will review typical challenges to a DLP deployment in an organization and how you can overcome them.

Mohan Atreya works in Product Management for RSA, The Security Division of EMC. His primary responsibility is to formulate the strategy for RSA's Data Loss Prevention (DLP) products. Mohan is a Certified Information Systems Security Professional (CISSP) and is the co-author of the book titled "Digital Signatures" published by McGraw-Hill/Osborne publications. He holds advanced degrees in Engineering from National University of Singapore.

***DLP in Theory and in Practice* - Pete Green, Novell**

DLP in Theory and in Practice: What We've Been Told, and...Reality. The cost and complexity of implementing a DLP solution has been vastly understated. Is the technology really as great as experts are telling us it is? In a word, yes.

Pete Green is a Certified Information Systems Security Professional (CISSP) with five years working with endpoint security and network access control. He has worked in IT for over 12 years in various systems and network administration capacities at organizations such as WordPerfect, Micron, PowerQuest, Symantec, and Senforce. Pete is currently a Novell Technical Specialist in End-user Computing and Systems Resource Management with Novell.

Safe Net

Join ISSA

To join the ISSA at https://www.issa.org/Join.html. General membership annual fee is $110; student fee $45 per year.